Malware

Dr. Talal Alkharobi

Malware (malicious software)

- Software Designed to infiltrate or damage a computer system without the owner's informed consent.
- The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.
- Many normal computer users are however still unfamiliar with the term, and most never use it.
- Instead, “virus” is used in common parlance and often in the general media to describe all kinds of malware.

Dr. Talal Alkharobi

3

Malware (malicious software)

- Another term that has been recently coined for malware is badware, perhaps due to the anti-malware initiative *Stopbadware* or corruption of the term "malware".
- Malware is sometimes known as a computer contaminant (law language)
- Malware should not be confused with defective software, that is, software which has a legitimate purpose but contains harmful bugs
- Software is considered malware based on the perceived intent of the creator rather than any particular features.

Dr. Talal Alsharekh

4

Types of Malware

- Computer viruses,
- Worms,
- trojan horses,
- Rootkit
- Ransomware
- Adware
- Spyware
- Botnets
- Key loggers
- Dialers

Dr. Talal Alsharekh

5

Infectious malware viruses and worms

- The best-known types of malware, viruses and worms, are known for the manner in which they spread, rather than any other particular behavior.
- Originally, the term computer virus was used for a program which infected other executable software, while a worm transmitted itself over a network to infect other computers.
- More recently, the words are often used interchangeably.
- Today, some draw the distinction between viruses and worms by saying that a virus requires user intervention to spread, whereas a worm spreads automatically.

Dr. Talal Alsharedah

6

computer virus

- A computer program that can copy itself and infect a computer without permission or knowledge of the user.
- The term comes from the term virus in biology.
- The original may modify the copies or the copies may modify themselves, as occurs in a metamorphic virus.
- A virus can spread from one computer to another when its host is taken to the uninfected computer, for instance by a user sending it over a network or carrying it on a removable medium.
- Some sources use virus as any form of self-replicating malware

Dr. Talal Alsharedah

7

computer virus

- Viruses may take advantage of network services such as the World Wide Web, e-mail, network/sharing file systems to spread
- Usually viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk.
- There are many viruses operating in the general Internet today, and new ones are discovered every day.

Dr. Talal Alsharedh

8

Why people create computer viruses

- Unlike biological viruses, computer viruses do not simply evolve by themselves.
- Computer viruses do not come into existence spontaneously, nor are they likely to be created by bugs in regular programs.
- They are deliberately created by programmers, or by people who use virus creation software.
- Computer viruses can only do what the programmers have programmed them to do.
- Virus writers can have various reasons for creating and spreading malware.

Dr. Talal Alsharedh

Why people create computer viruses

9

- Viruses have been written as
  - research projects,
  - pranks,
  - vandalism,
  - to attack the products of specific companies,
  - to distribute political messages,
  - financial gain from identity theft,
  - spyware,
  - cryptoviral extortion.

Dr. Talal Alsharedh

"Harmless" computer virus

10

- Some viruses are not designed to do any damage, but simply replicate themselves and perhaps make their presence known by presenting text, video, or audio, messages.
- Even these benign viruses can create problems for the computer user.
- They typically take up computer memory used by legitimate programs.
- As a result, they often cause erratic behavior and can result in system crashes.
- In addition, many viruses are bug-ridden, and these bugs may lead to system crashes and data loss.

Dr. Talal Alsharedh

11

Types of viruses

- Macro viruses
- Network viruses
- Logic bomb
- Cross-site scripting virus
- Sentinels
- Companion virus
- Boot sector viruses
- Multipartite viruses

Dr. Talal Alsharedh

12

Macro viruses

- A macro virus, often written in the scripting languages for programs such as Word and Excel, is spread by infecting documents and spreadsheets.
- Since macro viruses are written in the language of the application and not in that of the operating system, they are known to be platform-independent.
- They can spread between Windows, Mac and any other system, so long as they are running the required application.
- With the ever-increasing capabilities of macro languages in applications, and the possibility of infections spreading over networks, these viruses are major threats.

Dr. Talal Alsharedh

13

Macro viruses

- The first macro virus was written for Microsoft Word and was discovered in August 1995.
- Today, there are thousands of macro viruses in existence—some examples are Relax, Melissa.A and Bablas.

Dr. Talal Alsharedh

14

Network viruses

- This kind of virus is proficient in quickly spreading across a Local Area Network (LAN) or even over the Internet.
- Usually, it propagates through shared resources, such as shared drives and folders.
- Once it infects a new system, it searches for potential targets by searching the network for other vulnerable systems.
- Once a new vulnerable system is found, the network virus infects the other system, and thus spreads over the network.
- Some of the most notorious network viruses are Nimda and SQLSlammer.

Dr. Talal Alsharedh

15

Logic bomb

- A logic bomb employs code that lies inert until specific conditions are met.
- The resolution of the conditions will trigger a certain function such as printing a message to the user and/or deleting files.
- Logic bombs may reside within standalone programs, or they may be part of worms or viruses.
- An example of a logic bomb would be a virus that waits to execute until it has infected a certain number of hosts.
- A time bomb is a subset of logic bomb, which is set to trigger on a particular date and/or time.
- Example of a time bomb is the infamous 'Friday the 13th' virus.

Dr. Talal Alkharobi

16

Cross-site scripting virus

- A cross-site scripting virus (XSSV) is a type of virus that utilizes cross-site scripting vulnerabilities to replicate.
- A XSSV is spread between vulnerable web applications and web browsers creating a symbiotic relationship

Dr. Talal Alkharobi

17

Sentinels

- A sentinel is a highly advanced virus capable of empowering the creator or perpetrator of the virus with remote access control over the computers that are infected.
- They are used to form vast networks of zombie or slave computers which in turn can be used for malicious purposes such as a Distributed Denial of Service attack.

Dr. Talal Alsharedh

18

Companion virus

- A companion virus does not have host files per se, but exploits MS-DOS.
- A companion virus creates new files (typically .COM but can also use other extensions such as ".EXD") that have the same file names as legitimate .EXE files.
- When a user types in the name of a desired program, if a user does not type in ".EXE" but instead does not specify a file extension, DOS will assume he meant the file with the extension that comes first in alphabetical order and run the virus.
- For instance, if a user had "(filename).COM" (the virus) and "(filename).EXE" and the user typed "filename", he will run "(filename).COM" and run the virus.

Dr. Talal Alsharedh

19

Companion virus

- The virus will spread and do other tasks before redirecting to the legitimate file, which operates normally.
- Some companion viruses are known to run under Windows 95 and on DOS emulators on Windows NT systems.
- Path companion viruses create files that have the same name as the legitimate file and place new virus copies earlier in the directory paths.
- These viruses have become increasingly rare with the introduction of OSs in which you don't need to use the MS-DOS command prompt (Windows XP)

Dr. Talal Alsharedah

20

Boot sector viruses

- A boot sector virus alters or hides in the boot sector, usually the 1st sector, of a bootable disk or hard drive.
- The boot sector is where your computer starts reading your operating system.
- By inserting its code into the boot sector, a virus guarantees that it loads into memory during every boot sequence.
- A boot virus does not affect files; instead, it affects the disks that contain them.
- In the 1980s boot sector viruses were common and spread rapidly from one computer to another on rewritable floppy disks which contained programs.

Dr. Talal Alsharedah

21

Boot sector viruses

- With the CD-ROM revolution, it became impossible to infect read-only CDs.
- Though boot viruses still exist, they are much less common than in the 1980s.
- Additionally, modern operating systems do not allow ordinary programs to write to the boot sector.
- Examples of boot viruses are Polyboot.B and AntiEXE.

Dr. Talal Alsharedh

22

Multipartite viruses

- Multipartite viruses are a combination of boot sector viruses and file viruses.
- These viruses come in through infected media and reside in memory then move on to the boot sector of the hard drive.
- From there, the virus infects executable files on the hard drive and spreads across the system.
- There aren't too many multipartite viruses in existence today, but in the 1980s, they accounted for some major problems due to their capacity to combine different infection techniques.
- A well-known multipartite virus is Ywinz.

Dr. Talal Alsharedh

23

Computer worms

- A self-replicating computer program.
- It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention.
- Unlike a virus, it does not need to attach itself to an existing program.
- Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

Dr. Talal Alkharobi

24

Type of Worms

- Email Worms
- Instant messaging worms
- IRC worms
- File-sharing networks worms
- Internet Worms

Dr. Talal Alkharobi

25

Email Worms

- Spread via email messages.
- Typically the worm will arrive as email, where the message body or attachment contains the worm code, but it may also link to code on an external website.
- Poor design aside, most email systems requires the user to explicitly open an attachment to activate the worm, but "social engineering" can often successfully be used to encourage this;
- Once activated the worm will send itself out using either local email systems (e.g. MS Outlook services, Windows MAPI functions), or directly using SMTP.

Dr. Talal Alkharobi

26

Email Worms

- The addresses it sends to are often harvested from the infected computers email system or files.
- Worms using SMTP typically fake the sender's address

Dr. Talal Alkharobi

27

Instant messaging worms

- The spreading used is via instant messaging applications by sending links to infected websites to everyone on the local contact list.
- The only difference between these and email worms is the way chosen to send the links.

Dr. Talal Alkharobi

28

IRC worms

- Chat channels are the main target and the same infection/spreading method is used as above — sending infected files or links to infected websites.
- Infected file sending is less effective as the recipient needs to confirm receipt, save the file and open it before infection will take place.

Dr. Talal Alkharobi

29

File-sharing networks worms

- Copies itself into a shared folder, most likely located on the local machine.
- The worm will place a copy of itself in a shared folder under a harmless name.
- Now the worm is ready for download via the P2P network and spreading of the infected file will continue.

Dr. Talal Alsharedah

30

Internet Worms

- Those which target low level TCP/IP ports directly, rather than going via higher level protocols such as email or IRC.
- A classic example is "Blaster" which exploited a vulnerability in Microsoft's RPC.
- An infected machine aggressively scans random computers on both its local network and the public Internet attempting an exploit against port 135 which, if successful, spreads the worm to that machine.

Dr. Talal Alsharedah

31

Trojan horse

- A program that contains or installs a malicious program
- The term is derived from the classical Trojan Horse.
- Trojan horse programs cannot operate autonomously, the victim must activate them.
- As such, if trojans replicate and even distribute themselves, each new victim must run the program/trojan.
- Therefore their virulence is of a different nature, depending on successful implementation of social engineering concepts rather than flaws in a computer system's security design or configuration.

Dr. Talal Alkharobi

32

Trojan horse

- Trojan horses may appear to be useful or interesting programs (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed.
- There are two common types of Trojan horses.
  - Useful software that has been corrupted by a cracker inserting malicious code that executes while the program is used.
  - Standalone program that masquerades as something else, like a game or image file, in order to trick the user into some misdirected complicity that is needed to carry out the program's objectives.

Dr. Talal Alkharobi

33

rootkit

- A set of software tools intended to conceal running processes, files or system data from the operating system.
- Rootkits have their origin in relatively benign applications, but in recent years have been used increasingly by malware to help intruders maintain access to systems while avoiding detection.
- Rootkits exist for a variety of operating systems, such as Linux, Solaris and versions of Microsoft Windows.
- Rootkits often modify parts of the operating system or install themselves as drivers or kernel modules.

Dr. Talal Alkharobi

34

Ransomware

- A type of malware that uses a weak (breakable) cryptosystem to encrypt the data belonging to an individual, demanding a ransom for its restoration.
- This type of ransom attack can be accomplished by attaching a specially crafted file/program to an e-mail message and sending this to the victim.
- If the victim opens/executes the attachment, the program encrypts a number of files on the victim's computer.
- A ransom note is then left behind for the victim.
- The victim will be unable to open the encrypted files without the correct decryption key.

Dr. Talal Alkharobi

35

Ransomware

- Once the ransom demanded in the ransom note is paid, the cracker will (supposedly) send the decryption key, enabling decryption of the "kidnapped" files.
- However, if the decryption key is in the file/program then it can be extracted and used without contacting the attacker.

Dr. Talal Alsharedah

36

Adware

- advertising-supported software is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.
- It is usually seen by the programmer as a way to recover programming development costs, and in some cases it may allow the program to be provided to the user free of charge or at a reduced price.
- The advertising income may allow or motivate the programmer to continue to write, maintain and upgrade the software product.
- Some adware is also shareware, and so the word may be used as term of distinction to differentiate between types of shareware software

Dr. Talal Alsharedah

37

Adware

- What differentiates adware from other shareware is that it is primarily advertising-supported.
- Users may also be given the option to pay for a "registered" or "licensed" copy to do away with the advertisements.
- There are concerns about adware because it often takes the form of spyware, in which information about the user's activity is tracked, reported, and often re-sold, often without the knowledge or consent of the user.
- It may interfere with the function of other software applications, in order to force users to visit a particular web site.

Dr. Talal Alkharobi

38

Spyware

- a computer software that collects personal information about users without their informed consent.
- Personal information is secretly recorded with a variety of techniques, including logging keystrokes, recording Internet web browsing history, and scanning documents on the computer's hard disk.
- Purposes range from overtly criminal (theft of passwords and financial details) to the merely annoying (recording Internet search history for targeted advertising, while consuming computer resources).
- Spyware may collect different types of information. Some variants attempt to track the websites a user visits and then send this information to an advertising agency.

Dr. Talal Alkharobi

39

Spyware

- Number of companies have incorporated forms of spyware into their products.
- These programs are not considered malware, but are still spyware as they watch and observe for advertising purposes.
- It is debatable whether such 'legitimate' uses of adware/spyware are malware since the user often has no knowledge of these 'legitimate' programs being installed on his/her computer and is generally unaware that these programs are infringing on his/her privacy.
- In any case, these programs still use the resources of the host computer without permission.

Dr. Talal Alkharobi

40

Spyware

- More malicious variants attempt to intercept passwords or credit card numbers as a user enters them into a web form or other applications.

Dr. Talal Alkharobi

41

Botnet

- A collection of software robots, or bots, which run autonomously. This can also refer to the network of computers using distributed computing software.
- While the term "botnet" can be used to refer to any group of bots, such as IRC bots, the word is generally used to refer to a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.
- A botnet's originator can control the group remotely, usually through a means such as IRC, and usually for nefarious purposes. Individual programs manifest as IRC "bots".

Dr. Talal Alkharobi

42

Botnet

- Often the command and control takes place via an IRC server or a specific channel on a public IRC network.
- A bot typically runs hidden, and complies with the RFC 1459 (IRC) standard.
- Generally, the perpetrator of the botnet has compromised a series of systems using various tools (exploits, buffer overflows, as well as others; see also RPC).
- Newer bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords.
- Generally, the more vulnerabilities a bot can scan and propagate through, the more valuable it becomes to a botnet controller community.

Dr. Talal Alkharobi

43

Botnet

- Botnets have become a significant part of the Internet, albeit increasingly hidden.
- Due to most conventional IRC networks taking measures and blocking access to previously-hosted botnets, controllers must now find their own servers.
- Often, a botnet will include a variety of connections, ranging from dial-up, ADSL and cable, and a variety of network types, including educational, corporate, government and even military networks.
- Sometimes, a controller will hide an IRC server installation on an educational or corporate site, where high-speed connections can support a large number of other bots.

Dr. Talal Alkharobi

44

Botnet

- Exploitation of this method of using a bot to host other bots has proliferated only recently, as most script kiddies do not have the knowledge to take advantage of it.
- Several botnets have been found and removed from the Internet.
- The Dutch police found a 1.5 million node botnet and the Norwegian ISP Telenor disbanded a 10,000 node botnet.
- Large coordinated international efforts to shutdown botnets have also been initiated.
- It has been estimated that up to one quarter of all personal computers connected to the internet are part of a botnet.

Dr. Talal Alkharobi

45

Keystroke logging

- A diagnostic used in software development that captures the user's keystrokes.
- It can be useful to determine sources of error in computer systems
- Used to measure employee productivity on certain clerical tasks.
- Useful for law enforcement
- Spying; obtaining passwords or encryption keys
- Keyloggers are widely available on the internet and can be used by anyone for the same purposes.

Dr. Talal Alsharekh

46

Keyloggers Prevention

- Currently there is no easy way to prevent keylogging.
- The best strategy is to use common sense and a combination of several methods.
- **Monitoring** what programs are running: Users should constantly observe the programs which are installed on his machine.
- **Anti-spyware**: Anti-spyware applications are able to detect many keyloggers and cleanse them. Responsible vendors of monitoring software support detection by anti-spyware programs, thus preventing abuse of the software.

Dr. Talal Alsharekh

47

Keyloggers Prevention

- **Firewall**: Enabling a firewall does not stop keyloggers but can possibly prevent transmission of the logged material over the net.
- **Network monitors**: can be used to alert the user whenever an application attempts to make a network connection. This gives the user the chance to prevent the keylogger from "phoning home".

Dr. Talal Alsharedah

48

Keyloggers Prevention

- **Automatic form filler**: Automatic form-filling programs can prevent keylogging entirely by not using the keyboard at all.
  - Form fillers are primarily designed for web browsers to fill in checkout pages and log users into their accounts.
  - Once the user's account and credit card information has been entered into the program, it will be automatically entered into forms without ever using the keyboard or clipboard

Dr. Talal Alsharedah

49

Keyloggers Prevention

- **Alternative Keyboard Layouts**
  - Most keylogging hardware/software assumes that a person is using the standard QWERTY keyboard layout, by using a layout such as DVORAK captured keystrokes are nonsense unless converted.
  - For additional security custom keyboard layouts can be created using tools like the Microsoft Keyboard Layout Creator.
- On-screen keyboards, Web-based keyboard

Dr. Talal Alkharobi

50

Keyloggers Prevention

- It is important to generate **passwords** in a fashion that is invisible to keyloggers and screenshot utilities.
  - Using a browser integrated form filler and password generator that does not just pop up a password on the screen is therefore key.
  - Programs that do this can generate and fill passwords without ever using the keyboard or clipboard.

Dr. Talal Alkharobi

51

Dialer

- One way of stealing money from the infected PC owner is to take control of the modem and dial an expensive toll call.
- Dialer software dials up a premium-rate telephone number such as a "900 number" and leave the line open, charging the toll to the infected user.

Dr. Talal Alsharekh

52

Vulnerability to malware

- Homogeneity – e.g. when all computers in a network run the same OS, if you can break that OS, you can break into any computer running it.
- Bugginess – most systems containing errors which may be exploited by malware.
- Unconfirmed code – code from a floppy disk, CD or USB device may be executed without the user's agreement.
- Over-privileged users – some systems allow all users to modify their internal structures.
- Over-privileged code – most popular systems allow code executed by a user all rights of that user.

Dr. Talal Alsharekh